WP 可解公式上警示传播算法收敛的有效条件 *

崔　立，王晓峰，牛　进

(北方民族大学 计算机科学与工程学院，银川 750021)

摘　要：信息传播算法求解可满足性问题时非常有效，警示传播（warning propagation，WP）算法是最为基础的信息传播算法。通过对 WP 算法的数学原理分析，高概率确定的部分变元与公式的骨干集合后门集有密切关系。针对 WP 算法收敛性的研究，基于骨干集和后门集定义 WP-可解公式，利用在 G(n, 3, m)模型和植入指派模型下证明 WP 算法的收敛性，给出算法收敛的充要条件。最后，通过在植入指派的公式产生模型上进行数值实验验证，结果表明：如果一个可满足性公式 WP-可解公式，当且仅当 WP 算法高概率收敛。

关键词：警示传播算法；骨干集；后门集；WP-可解公式；实例产生模型

中图分类号：TP　　doi: 10.19734/j.issn.1001-3695.2018.11.0791

Effective conditions for warning propagation algorithm convergence on WP solvable formula

Cui Li, Wang Xiaofeng, Niu Jin

(*School of Computer Science & Engineering*, *North Minzu University*, *Yinchuan* 750021, *China*)

Abstract: It is very effective when the message passing algorithm solves the satisfiability problem, while the most basic message passing algorithm is the warning propagation (WP) algorithm. Through the analysis of the mathematical principle of WP algorithm, it could be found that the partial variables determined by high probability are closely related to the backbone set and backdoor set of the formula. For the study of the convergence of WP-solvable formula and WP algorithm, WP-solvable formula was defined based on backbone set and backdoor set, and by using the G(n, 3, m) model and the planted distribution model to prove the convergence of the WP algorithm, the necessary and sufficient conditions for the convergence of the algorithm are given. Finally, by carrying out the numerical experiments on the model of the planted distribution formula, The results show that if a satisfiability formula WP-solvable formula, if and only if the WP algorithm has a high probability of convergence.

Key words: warning propagation algorithm; backbone; backdoor; WP-solvable formula; instance generation mode

0　引言

约束可满足性问题（constraint satifiability problem，CSP）是人工智能中一个重要的研究领域[1~3]，*SAT* (satisfiability)问题是典型的 *CSP* 问题[4~6]。*SAT* 问题的 *NP* -完全性表明，不存在多项式时间算法求解该问题。然而现实世界中很多复杂问题通过编码都可以转换为 *SAT* 问题，如机器人路径规划问题、智能系统知识推理、大型复杂系统控制等。尽管 *SAT* 问题是 *NP* -难的，随着研究的不断深入以及硬件的发展，*SAT* 问题求解器越来越智能，使得难解区域变窄，甚至能够在多项式时间内求解变相点附近的难解实例。梳理这几年的研究成果，*SAT* 问题研究主要集中在两个方面，一方面，通过构造实例产生模型，分析该问题的相变现象。最具有代表性的是随机 3−*SAT* 实例产生模型 $G(n,3,m)$，该模型中子句与变元的比值 $\alpha=m/n$ 是一个重要的参数，它不仅仅影响实例的可满足性，而且影响实例的判定难度[7]。随机统计现象表明，对于随机 3−*SAT* 实例产生模型 $G(n,3,m)$，存在可满足的相变点 α_d。当 $\alpha<\alpha_d$ 时，实例高概率可满足；当 $\alpha>\alpha_d$ 时，实例高概率的不可满足[8]。把满足与不可满足之间出现的这种临界现象称为相变现象。α_d 称为相变点，在相变点附近区域的实例求解难度较大。尽管人们不知道 α_d 的确切值，但研究表明，α_d 至少为 3.52[9]，至多为 4.4898[10]。在该模型中通过控制参数 α 来构造实例，大量的实验研究表明，当 α 的值大约在 4.27 附近时，产生的实例求解难度最大。Xu 等人[11,12]分别在 B 模型和 D 模型的基础上提出了具有精确相变点的 RB 模型和 RD 模型，解决了经典 *CSP* 实例产生模型的平凡无解性问题，被广泛用于构造 *CSP* 问题和 *SAT* 问题的难解实例。

另一方面，设计更加有效的求解 *SAT* 问题的判定算法[13]。大多数 *SAT* 问题求解算法利用了隐藏在实例内部的某种特殊结构，较大程度地提高了算法的搜索能力，而骨干集和后门集是 *SAT* 实例中最为重要的结构，在算法求解过程中起关键性作用。Monasson 和 Silliams 等人在研究可满足性问题的相变现象和复杂度时，首次提出了骨干集和后门集的概念[14]。骨干集和后门集都与问题的难度相关，骨干集越大，问题的难度越大；同样，后门集越大，问题的难度越大[15]。事实上，对于一些结构化的实例，骨干集和后门集有一定联系[16~20]，现实世界中许多具有结构化的 *SAT* 问题都有较小的骨干集和后门集，一些著名的搜索算法利用了这种结构特征，求解这些实际问题往往比求解随机 3−*SAT* 更为有效[14]。

在 *SAT* 问题判定算法的研究中，人们发现实例的隐藏结

收稿日期：2018-11-20；**修回日期：**2019-01-15　**基金项目：**国家自然科学基金资助项目（61462001，61762019，61762002，11761002，61561002）；北方民族大学重点科研项目（2017KJ24，2017KJ25）；2018 宁夏回族自治区重点研发计划项目（2018BEE03019）；宁夏高等学校一流学科建设（电子科学与技术学科）资助项目（NXYLXK2017A07）

作者简介：崔立（1994-），男，陕西宝鸡，硕士研究生，主要研究方向为算法分析与设计；王晓峰（1980-），男，甘肃会宁人，副教授，博士，主要研究方向为机器学习、算法分析与设计（xfwang@nun.edu.cn）；牛进（1993-），男，陕西安康，硕士研究生，主要研究方向为人工智能.

构对算法的性能有影响，最为重要的隐藏结构主要有骨干集和后门集。骨干集是文字的集合，指对于一个可满足命题公式的每一个真值指派使得骨干集中的文字均为真；后门集是变元的集合，指对后门集中的变元赋值后将相应的命题公式化简为易解公式，即多项时间可解公式（如 $HORN$ 、$2-SAT$ 公式等）。骨干集的大小与问题的难度有关，直观上骨干集越大，SAT 问题求解难度越大，原因在于骨干集增大，解被聚类的可能性增大，可灵活赋值的变元相对减少，公式被容易错误赋值的概率增大，增加了局部搜索算法的求解难度，这也解释了在可满足相变点附近公式的求解难度较大。类似地，从后门集的定义可以看出，后门集越大，问题判定的难度越大。后门集与求解算法有关，不同的求解算法可能有不同的后门集，而骨干集与问题本身有关，每个 SAT 实例有唯一的骨干集。根据定义不难看出，骨干集与后门集之间没有必然的联系，后门集与骨干集的重叠部分很小。

20 世纪 80 年代，物理学家提出了一种基于消息传递的信息传播算法，数值实验证明该算法求解组合优化问题时非常有效[21]，被广泛应用于人工智能和工程技术等各个领域。在文献[22]中设计了三种求解随机 $3-SAT$ 问题的信息传播算法，分别为警示传播（warning propagation，WP）算法、信念传播（belief propagation，BP）算法、调查传播（survey propagation,SP）算法，其中 WP 算法能够求解子句数与变元数的比值 $\alpha<3.5$ 的随机实例。

但是当 $\alpha>3.5$ 时，WP 算法常表现为不收敛，在实验数据中会发现这种现象，却对于这种不收敛现象，缺少一定的系统理论解释。所以，对于研究信息传播算法的收敛性具有重要意义。信息传播算法的特征在于基于消息传播可以将一个满足指派的部分变元取值以高概率确定，从而可以将公式简化。经过多次操作，如果能够将公式化简为易解公式，则调用某个求解 SAT 问题的算法对公式进行求解。特别是基于 WP 算法“冻结”的部分变元，这些变元以概率为 1 力迫取某个固定值，也就是说某些子句的可满足性完全由这些被“冻结”的变元取值决定。本文的主要工作是，由骨干集和后门集的定义，提出了 $WP-$ 可解公式的定义。通过对该公式的结构进行分析，给出了基于 $WP-$ 可解公式上警示传播算法收敛的一个有效条件。

1 命题公式的特殊变元集

骨干（backbone）：设 F 为一个 CNF 公式，其变元集 $\mathrm{var}(F)=\{x_1,\cdots,x_n\}$，一个变元子集 $S\subseteq \mathrm{var}(F)$ 称为 F 的骨干变元集，简称 F 的骨干(backbone)。如果 $F\models \wedge Lit(S)$，即任意一个使 F 为真的赋值 τ，都使得 $Lit(S)$ 中的文字为真。换言之，每一个使 F 为真的真值指派 τ，在变元集 S 上的赋值是固定的。其中 $Lit(S)=\{L_{1,\ldots\ldots,}L_{|S|}\}$ 为由 S 内的每个变元取正（或负）文字得到，文字合取 $\wedge Lit(S)=(L_1\wedge\ldots\ldots\wedge L_{|S|})$。

后门集（backdoor）：设 F 为一个 CNF 其变元集 $\mathrm{var}(F)=\{x_{1,\ldots\ldots,}x_n\}$，$C$ 是一个易解类，即可满足性判定问题在多项式时间内可解。

一个变元子集 $S\subseteq \mathrm{var}(F)$ 称为 $C-$ 弱后门集（weak backdoor），如果存在对 S 上变元的任意一个赋值 τ_s 下简化为 C 类中的一个公式。

一个变元子集 $S\subseteq \mathrm{var}(F)$ 称为 $C-$ 强后门集（strong backdoor），如果对于 S 上变元的一个赋值 τ_s，公式在赋值 τ_s 下简化为 C 类中的一个公式。

一般地，变元子集 $S\subseteq \mathrm{var}(F)$ 称为 F 的一个弱后门集，如果存在对 S 上变元的一个赋值 τ_s，公式 F 在赋值 τ_s 下简化为一个易解公式。一个变元子集 $S\subseteq \mathrm{var}(F)$ 称为强后门集，如果对于 S 上变元的任意一个赋值 τ_s，公式 F 在赋值 τ_s 下化简为一个容易可解公式。

警示传播（warning propagation，WP）算法中的信息取值为 1 或 0。子句节点 c 传递给变元节点 i 的值为 1 隐示，子句 c 中除变元 i 外的所有变元均以概率为 1“力迫”一个事实：子句 c 的可满足性完全依赖于变元 i 的取值。换句话说，变元 i 的取值被固定（冻结）,已经知道：对于 WP 算法，因子图为树结构的公式（简称树公式）容易求解。根据信息传播算法这样的机理，公式的骨干集与公式关于易可解类的后门集密切相关。

由骨干集的定义可知，$|S|$ 越大，公式化简到易可解类的可能性就越大；反之，$|S|$ 越小，WP 算法中每一轮更新化简公式的效果就越差。本文相信：在 WP 算法下仍然难解的公式与其骨干集和后门集的大小和分布密切相关，这就隐约告诉人们：WP 算法冻结的变元与骨干集和后门集中的变元有关系。基于此，本文引入 WP—可解的概念。

1.1 *WP*-可解公式

一个 CNF 公式 F 成为 WP-可解公式，如果存在变元集 $X=(x_1,x_2,\ldots,x_n)$ 的子集 $S_1,S_2,\ldots,S_m$ 满足如下条件：

a） S_1 是 $F_0=F$ 的骨干集，且对应于一个 S_1 上的文字集合 $Lit(S_1)$ 规定的部分赋值 τ_{S_1}，在此赋值下得到 $F_0|_{\tau_{S_1}}=F_1$；

b）对 $2\le k\le m$，S_k 是 F_{k-1} 的骨干集，且对应于一个 S_k 上的文字集合 $Lit(S_k)$ 规定的部分赋值 τ_{S_k}，在此赋值下得到 $F_{k-1}|_{\tau_{S_k}}=F_k$；

c） F_m 是一个易解公式。

显然，树公式是 WP-可解公式。

$3CNF$ 公式是子句 $C_1,C_2,\ldots,C_n$ 合取结果，其中每个子句是三个文字析取的结果，每个文字都是一个变量或者变量的否定，一个文字对应变量 x_1 或对应变量的否定 $\neg x_1$。如果对变量进行布尔赋值，则 $3CNF$ 是可满足的，每个子句至少包含一个计算结果为 $true$ 的文字。$3SAT$ 是所有了满足 $3CNF$ 公式的语言。

1.2 植入指派（planted distribution）

近年来，随机结构的算法理论一直是广泛研究的焦点。众所周知，$3SAT$ 在子句与变量的比率方面有一个明显令人满意的阈值。即随机 $3CNF$ 的子句与变量的比率低于阈值的时，这时候是高概率（with high probability，whp）满足；当子句与变量的比率高于阈值时，这时候是高概率不满足。这个阈值并不是已知的，甚至都不知道这个阈值是一个常量，但是目前已知的最佳界限至少是 3.42，最多是 4.5。在这样的比例，大多数的公式都不能满足，分析随机可满足实例的分布似乎很困难。因此本文关注 $3-SAT$ 植入分布，用 $P_{n,p}^{plant}$ 表示[23]。

该分布中的随机 $3CNF$ 是通过对变量选择赋值 φ，然后包括 φ 满足的子句以概率 $p=p(n)$ 来获得，从而保证得到的实例是可满足的。具体地讲，由随机选择一个赋值 x 均匀地分布在 $\{0,1\}^n$ 的 2^n 元素中，然后独立选择 x 满足的 $(2^k-1)\binom{n}{k}$ 子句中的所有子句生成。每个子句以均匀随机顺序的 k 文字给出。（n 是变量的个数，k 是每个子句中包含变量的个数）。

在 $P_{n,p}^{plant}$ 中植入的实例是随机选择 n 个变量的真值赋值生成的，φ 满足的每个子句都包含在概率 p 中。在这个工作中本文要考虑 $p\ge d/n^2$，其中 d 是足够大的常数[24,25]。本文着重研究随机 $3CNF$ 问题，在植入分布的随机 $3CNF$ 公式，以高概

率 p 满足每个子句，从而保证得到的实例 F 是可满足的。由植入分布的定义可以知道，当概率 p 足够大时，$p_{n,p}^{plant}$ 产生的实例 F 高概率的只有一个可满足解。

2　WP 算法

2.1　因子图

设 $F=\{C_1,C_2,\ldots,C_m\}$ 为一个 CNF 公式，含有 n 个变元 $x_1,x_2,\ldots x_n$，用 i 代表变元 x_i。公式 F 可以用一个二分图 $G=\{C\cup X,E\}$ 表示，称为因子图。其中，变元节点集 $X=\{1,2,\ldots,n\}$，子句节点集为 $C=\{C_1,C_2,\ldots,C_m\}$。图 G 中的边分为两类：实边和虚边[26]。

实边：$(C_i,j)\in E \Leftrightarrow$ 子句 C_i 含正文字 x_j；

虚边：$(C_i,j)\in E \Leftrightarrow$ 子句 C_i 含负文字 x_j。

一个 SAT 问题可以转换为因子图来表示，如图 1 所示。每个 N 变量与图中的顶点相关，被称为变量节点（在图中用圈表示），每个 M 子句都与图中的另一种顶点相关联，被称为功能节点（在图中用方框表示）。当变量 x_i 出现在子句 A 中时，功能节点 A 通过一条边与变量节点连接；当子句中出现的变量为 x_i 时，a 与 i 之间用实线（$J_i^a=-1$）；当子句中出现的变量为 $\neg x_i$ 时，a 与 i 之间用虚线（$J_i^a=1$）。变量节点构成的集合 X（$|X|=N$），功能节点的集合 A（$|A|=M$）。

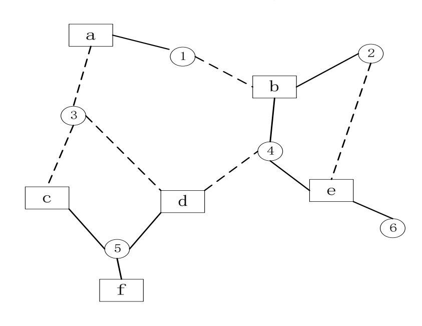


图 1　因子图

Fig. 1　Factor diagram

一个因子图里面有六个变量节点 $i=1,\ldots,6$，六个功能节点 a,b,c,d,e,f，则这个公式可以写为

$$F=(x_1\vee\neg x_3)\wedge(\neg x_1\vee x_2\vee x_4)\wedge(\neg x_3\vee x_5)\wedge$$
$$(\neg x_3\vee\neg x_4\vee x_5)\wedge(\neg x_2\vee x_4\vee x_6)\wedge(x_6)$$

2.2　*WP* 算法

一个 CSP 问题是一个三元组 $\langle X,D,C\rangle$，其中：表示变量的集合，记为 $X=\{x_1,\ldots,x_m\}$；D 是关于变量 $x_1,\ldots,x_m$ 的取值域的集合，记为 $D=\{D_1,\ldots,D_m\}$；C 是约束的集合，每一个约束 $c=\langle\sigma,\rho\rangle$。其中：约束范围 σ 是变量的列表；约束关系 ρ 是关于 σ 中变量取值域的笛卡尔积的子集。可满足性问题判定（SAT）是典型的 CSP 问题，即给定一个合取范式（conjunctive normal form,CNF）F，SAT 判定问题指是否存在一组指派使得 F 为真[27]。

$V(a)$：表示出现在子句 a 中的变元集合，$V(a):=V^+(a)\cup V^-(a)$。其中，$V^+(a)$：表示出现在子句 a 中的正文字对应的变元标志集合。

$V^-(a)$:表示出现在子句 a 中的负文字对应的变元标志集合。

$V(a)\backslash i:=V(a)-\{i\}$。

$V(j)$:表示含变元 x_j 中的子句集合，$V(j):=V^+(j)\cup V^-(j)$。其中：$V^+(j)$:表示变元 x_j 正出现的子句集合。

$V^-(j)$:表示变元 x_j 负出现的子句集合。$V(j)\backslash a:=V(j)-\{a\}$。

J_j^a 是一个标志参数，若 x_i 出现在子句 a 中，则 $J_j^a=-1$；若 $\neg x_i$ 出现在子句 a 中，则 $J_j^a=1$。在因子图的每条边 (a,i) 上，定义 WP 算法中的消息传递 $u_{a\to i}$（常称为警示信息）。$u_{a\to i}$ 表示子句 a 的可满足性对变元 x_i 的取值倾向。WP 算法的消息更新迭代方程如下：

$$u_{a\to i}(t)=\prod_{j\in V(a)\backslash i}\theta\left(-J_j^a\left(\sum_{b\in V(j)\backslash a}J_j^b u_{b\to j}(t-1)\right)\right) \tag{1}$$

其中：t 表示迭代次数；$\theta(x)$ 是截尾函数，如果 $x\le 0$，则 $\theta(x)=0$，否则 $\theta(x)=1$。若 a 中仅包含变元 x_i，则置 $u_{a\to i}=1$。当 WP 算法收敛时，根据警示信息固定变元 x_i 的赋值。

$$H_i=-\sum_{b\in V(j)}J_i^b u_{b\to i}^* \tag{2}$$

如果 $H_i>0$，则 $x_i=1$；如果 $H_i<0$，则 $x_i=0$；否则 x_i 暂且不赋值。一般地将式（1）改写为

$$u_{a\to i}(t)=\prod_{j\in V(a)\backslash i}\theta\left(-J_j^a\left(\sum_{b\in V^+(j)\backslash a}u_{b\to j}(t-1)-\sum_{b\in V^-(j)\backslash a}u_{b\to j}(t-1)\right)\right) \tag{3}$$

$$h_{j\to a}=\sum_{b\in V^+(j)\backslash a}u_{b\to j}(t-1)-\sum_{b\in V^-(j)\backslash a}u_{b\to j}(t-1) \tag{4}$$

称 $h_{j\to a}$ 为腔域。若变元 x_j 仅出现在 a 中，则置 $h_{j\to a}=0$。求解 CNF 公式 F 的 WP（warning propagation）算法如下：

Warning propagation（CNF formula F）

构造相应的因子图 $G(F)$；

给因子图上的所有消息边 $u_{a\to i}(t=0)$ 随机赋值 0 或 1；

重复如下过程，直到算法收敛（可设置最大迭代步 $t_{\max}$ 强迫算法结束）：

对 $G(F)$ 中的边随机排列；

根据随机边序列，利用（1）式更新消息 $u_{a\to i}$；

根据 H_i，计算部分指派 ψ，对公式 F 进行简化；

返回 ψ。

3　WP 算法收敛的条件

由于 3−SAT 问题是 NP 难问题，在 $P\ne NP$ 条件下，不存在多项式时间算法求解该问题[28]。信息传播算法是目前求解 3−SAT 问题最为有效的办法，然而对于相变点附近的 3−SAT 实例，该算法不总有效，常表现为不收敛。但目前对信息传播算法的收敛性理论研究较少，研究也变得非常困难。

每一个使 F 为真的真值指派 τ，在变元集 S 上的赋值是固定的，在骨干集的集合之中每一个变量都可以使得公式 F 为真；后门集的集合之中，对公式 F 赋值之后，都可以使得公式 F 得到不同程度上的化简，最后化简为一个易解公式。因此在骨干集与后门集之间存下如下的关系，如图 2 所示：

若 S_1 表示骨干子集的集合；S_2 表示后门子集的集合，那么骨干集的集合 S_1 与后门集的集合 S_2 之间存在以下四种情况：

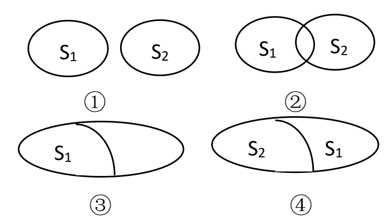


图 2　骨干集与后门集关系图

Fig. 2　Relationship between backbone set and backdoor set

图 2 中：①表示骨干集与后门集没有任何交集；②表示骨干集与后门集的部分集合是相同的，公共部分为 $S_1\cap S_2$；③表示在骨干集的集合中包含着后门集的集合，即 $S_2\subseteq S_1$，公共部分为后门集 S_2；④表示在后门集的集合中包含着骨干集的集合，即 $S_1\subseteq S_2$，公共部分为骨干集 S_1，称公共部分的变元为核变元，被该变元满足的子句称为支持子句。

根据 WP-可解公式的概念可以得出：只研究图中③这一种情况的类型。WP 算法收敛的时候，得到部分变元的赋值，该赋值是高概率，使得 WP-可解公式可满足，从而进一步说明，该变元赋值的改变使得在植入分布 $p_{n,p}^{plant}$ 模型下产生实例 F 是高概率不可满足，这就告诉本文：由 WP 算法收敛后确定的变元高概率的是骨干变元。因此，本文有如下定理：

定理 1　若合取范式（CNF）公式 F 为 WP-可解公式，当且仅当 WP 算法高概率收敛。

为了证明定理 1，现本文需要证明如下两个定理：定理 2　若 WP 算法收敛，则合取范式（CNF）公式 F 为 WP-可解公式；

证明　基于图③情况下对此定理进行研究分析。可满足性问题（SAT），例如 $3-SAT$，$k-SAT$ 等问题都是属于 NP 难问题，则产生的 $3-CNF$ 公式 F 是在多项式时间内无法求解

如果 WP 算法收敛，得到不动点 $u^*=\{u_{a\to i}^*:(a,i)\in E\}$。利用 $u^*=\{u_{a\to i}^*:(a,i)\in E\}$ 启发式定义每一个变量的取值，并对公式进行化简。如此重复，寻找到公式的满足性指派集合。根据骨干集的定义，本文将骨干的变元集记为 $D(F)$。本文有如下定理[29]：

设 F 为一个可满足的合取范式（CNF）公式，其变元集为 $\mathrm{var}(F)=\{x_1,x_2,\ldots,x_n\}$，假设 WP 算法关于输入 F 收敛，则变元集 $\{x_i:u_{a\to i}^*=1,(a,i)\in E\}$ 是 $D(F)$ 的一个子集，其中 $u^*=\{u_{a\to i}^*:(a,i)\in E\}$ 是 WP 算法得到的不动点。

假定一个可满足性的合取范式（CNF）公式为 F，输入公式 F 在 WP 算法中是收敛的，因此通过 WP 算法会得到一个固定点，即不动点 $u^*=\{u_{a\to i}^*:(a,i)\in E\}$。

假设 WP 算法在 n 步之内收敛，其中 $n\geq 1$，对 n 数学归纳，本文可以得到一个结果：若 $u_{c\to i}^*=1$，则子句 c 的可满足性完全依赖于变元 x_i 的取值。若 c 是一个单位子句，在 WP 算法中，$u_{c\to i}(1)=u_{c\to i}(2)=\cdots=u_{c\to i}(n)=1$。因为 CNF 公式 F 在 WP 算法中收敛，即 F 是可满足，对于所有的变量都存在 $\left(\sum_{c\in V_+(i)}u_{c\to i}^*\right)\left(\sum_{c\in V_-(i)}u_{c\to i}^*\right)=0$。

当 $c\in V_+(i)$ 且 $u_{c\to i}^*=1$ 时，则对于任意满足 F 的真值指派函数 v：$\mathrm{var}(F)\to\{0,1\}$，对于任何文字 $M\in c\setminus\{x_i\}$ 一定存在 $v(M)=0$，$v(x_i)=1$。同理，当 $c\in V_-(i)$ 且 $u_{c\to i}^*=1$ 时，则对于任意满足 F 的真值指派 v，对于任何文字 $M\in c\setminus\{\neg x_i\}$ 一定存在 $v(M)=0$，$v(\neg x_i)=1$。即：若 $u_{c\to i}^*=1$，出现在 c 中对应于变元 x_i 的文字是一个关键文字。因此，变元集 $\{x_i:u_{a\to i}^*=1,(a,i)\in E\}$ 是 $D(F)$ 的一个子集。

根据以上定理，引出一个求解公式的骨干变元集的算法，简称 *backbone* 算法。

backbone 算法:

Input：一个 CNF 公式 F 的因子图 $G=(V,E)$；

Output：输出公式不满足的状态标识 $UNSAT$，或者一个变元集 B；

初始化 $B=\phi$

While　存在不固定变元　*do*

　运行 WP 算法

　如果 WP 不收敛，则输出 B；否则计算所有 H_i 和冲突标识 b_i；

　如果存在某个 $b_i=1$，则输出 $UNSAT$；

　如果所有的 H_i 为 0，则输出 B；否则

　　While　$H_i\neq 0$　*do*

　　　当 $H_i>0$ 时，令 $x_i=1$；

　　　　$B=B\cup\{i\}$；

　　　当 $H_i<0$ 时，令 $x_i=0$；

　　　　$B=B\cup\{i\}$；

　　　对图进行清洗；（即，对公式进行简化）

　　Endwhile

　Endwhile

End

WP 算法是通过这些赋值对公式 F 进行化简，化简后的子公式上继续使用 WP 算法，通过多次迭代化简可以将一个公式 F 化简为易解公式，调用其他算法对该易解公式求解。如果 WP 算法收敛，可以得到警示信息的不动点 $u^*=\{u_{a\to i}^*:(a,i)\in E\}$，根据局部域 H_i 启发式定义每一变元的取值，并对公式进行化简。如此重复，寻找公式的满足指配。当冲突数 $c_i=1$ 时，表示变元取值冲突，公式是不可满足的；当 $c_i=0$ 时，利用 H_i 诱导变元赋值以高概率满足公式。对于树公式来说，如果 WP 算法收敛，可以通过 H_i 高概率的固定部分变元的取值，以此来简化公式。

在 WP 算法在关于公式 F 收敛之后，必然会产生部分变元赋值，这些变元的赋值都可以使得公式 F 得到满足，且这部分变元定是包含于骨干集之中。但是根据 WP-可解公式的定义可知：对 $2\leq k\leq m$，S_k 是 F_{k-1} 的骨干集，存在部分赋值，在这个赋值之下，$3-CNF$ 公式 F 是可以化简为一个易解公式，这个易解公式在多项式时间内必然是可解的，满足 WP-可解公式，因此可以得出：若 WP 算法收敛，则合取范式（CNF）公式 F 为 WP-可解公式。

定理 3　若合取范式（CNF）公式 F 为 WP-可解公式，则 WP 算法高概率收敛；

证明　基于图 2 中③情况下对此定理进行研究分析。对于植入分布模型来说，当 p 足够大时，高概率得存在一个赋值满足公式 F，所以，根据 WP—可解公式的概念，必然高概率得有骨干集变元包含在这个赋值。

在植入分布 $p_{n,p}^{plant}$ 模型下，如果 π 和 α 随机均匀选取，那么以概率 $1-e^{-\Omega(d)}$ 有 $\#H=(1-e^{-\Omega(d)})n$。其中：π 是一个子句变元边的序列；α 是子句变元边上的信息向量；H 表示核心变量（核变量）。这句话隐含：当 $p=c\log n/n^2$ 时，高概率地 H 包含了所有变元。由图 2 中③可知，核变元包含于骨干集之中，即在分布中，核变元所具有的特征，骨干变元也是具备的，由 WP-可解公式的概念，显然，树公式是一个 WP-可解公式。

若 F 为 WP-可解公式，则实例 F 中的变元满足对 $2\leq k\leq m$，S_k 是 F_{k-1} 的骨干集，且对应于一个 S_k 上的文字集合 $Lit(S_k)$ 规定的部分赋值 τ_{S_k}，在此赋值下得到 $F_{k-1}|_{\tau_{S_k}}=F_k$，即在骨干集的部分赋值之下，可以将公式 F 化简为一个易解公式，此公式可以在多项式时间内求解，以此可以使得原问题得到简化。在植入指派 $p_{n,p}^{plant}$ 模型中，当 p 足够大时，必然存在一组赋值 φ^* 使得公式 F 得到满足。再此之前，本文已得 WP 算法收敛情况下，确定的变元高概率的是骨干变元集，且骨干变元集高概率地包含于在这组赋值 φ^* 中。

在文献[24]中分析了植入指派的可满足性公式上警示传播算法的收敛性，给出了算法收敛的充分条件，有定理如下：

F 是一个由模型 $p_{n,p}^{plant}$ 产生的随机 3CNF 公式，$p\geq d/n^2$，d 是一个有效足够大常数。存在一个可满足性指派 φ^*，高概率有如下结论：

a）WP 在 F 上最多迭代 $O(\log n)$ 步收敛；

b）ψ 是 WP 返回的部分指派，V_A 是被赋值的变量集合，V_U 是未被赋值的变量集合。那么对于 $x\in V_A$，$\varphi(x)=\varphi^*(x)$，且 $\#V_A\geq(1-e^{-\Theta(d)})n$；

c）$F|_{\psi}$ 是一个简单公式，且能够在 $O(n)$ 实际内判定 。

上述定理是关于植入指派 $p_{n,p}^{plant}$ 模型的，对于随机实例产生模型 $G(m,k,n)$ 也成立。在植入指派 $p_{n,p}^{plant}$ 模型中，当 $k=n$ 时，此时子句的个数为 C_n^3，以高概率 p 满足子句的情况下，产生实例 F 的子句个数则为 $C_n^3 \bullet p$，其中 $C_n^3 \bullet p \le C_n^3$，在这些子句中，高概率的存在一组解使得实例 F 是可满足的。

因 WP-可解公式 F 最终可以化简为易解公式，且其中变元集高概率得为骨干集 $D(F)$，与 $p_{n,p}^{plant}$ 模型下高概率产生的解 φ^* 的关系是：$D(F) \subseteq \varphi^*$。由 $p_{n,p}^{plant}$ 模型下高概率结论可知：WP 在 F 上最多迭代 $O(\log n)$ 步收敛；$F|_{\psi}$ 是一个简单公式，且能够在 $O(n)$ 实际内判定。此证：F 为 WP-可解公式，则 WP 算法高概率收敛。　　□

至此，定理 1 证明完毕。

4　数值实验

因子句个数 m 随着变量数 n 的增大而呈指数级增长（2^n），因此在整个实验过程中变量数的大小取 n=3,4,5,6,7,8,9，10 得出所有可能性子句的个数和在高概率下（$p>0.8$）植入指派得到子句的个数，如图 3 和表 1 所示。在变量数不断变化的情况下，图 4~6 是变量数分别为 10、20、30 时，可满足性子句的收敛性情况；图 7~9 是变量数分别为 10、20、30，可正确判定实例图的概率。

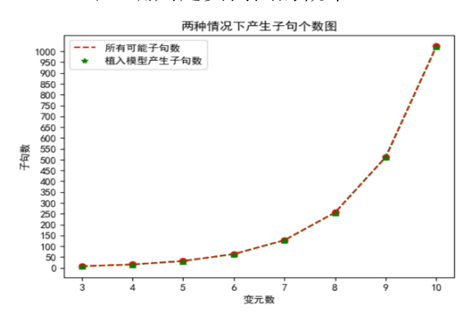


图 3　两种情况下的子句情况图

Fig. 3　Case diagram of two cases

表 1　子句个数

Table 1　Number of clauses

变元个数 n	子句所有可能个数	指派模型下子句数
3	8	7
4	16	15
5	32	31
6	64	63
7	128	127
8	256	255
9	512	511
10	1024	1023

图 4　n=10 的收敛性图

Fig. 4　Convergence graph of n=10

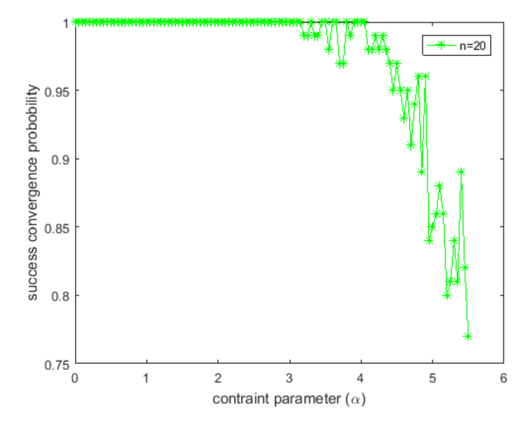


图 5　n=20 的收敛性图

Fig. 5　Convergence graph of n=20

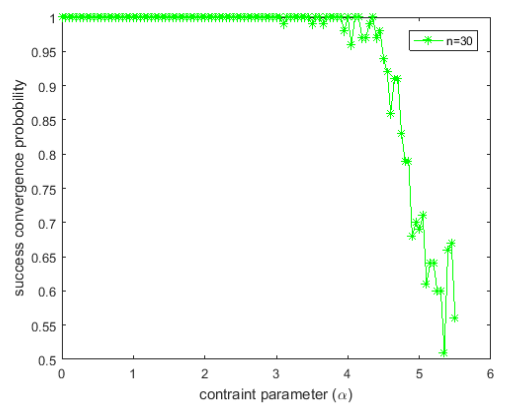


图 6　n=30 的收敛性图

Fig. 6　Convergence graph of n=30

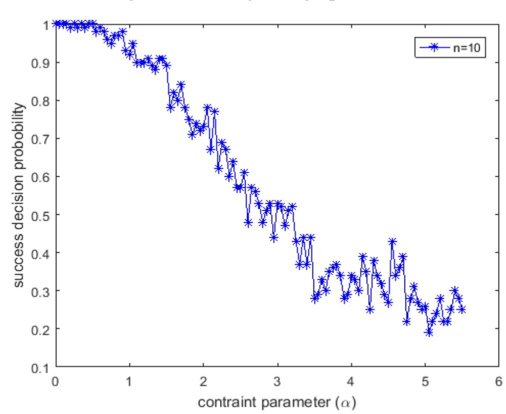


图 7　n=10 正确判定的实例图

Fig. 7　Example of n=10 correct decision

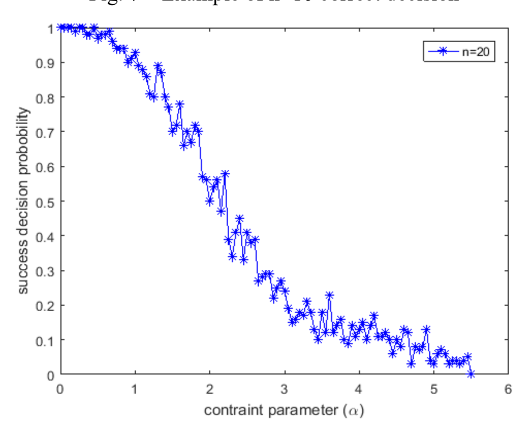


图 8　n=20 正确判定的实例图

Fig. 8　Example of n=20correct decision

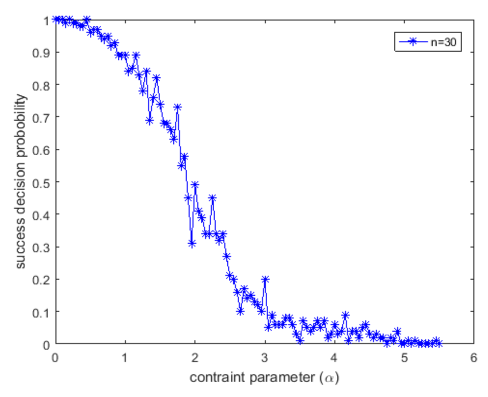


图 9 n=30，正确判定的实例图

Fig. 9 Example of n=30 correct decision

随着 n 的增加，产生子句的个数也增加，产生可满足性实例包含的子句也在增加，在变元 n 逐渐增大，算法在 $\alpha<3.5$ 收敛于 1，$\alpha>3.5$ 算法表现为不收敛，呈下降趋势。可正确判定实例的概率也随着 n 的增大呈离散的分布，即当迭代次数较小的时候，可判定实例的概率趋于 1，随着迭代次数的增加，可判定实例的概率趋于减小。

从实验的数据中，在 *WP* 算法迭代 1 000 次之后，可满足公式 *F* 中包含的子句必然包含于在高概率 $p>0.8$ 的情况下，产生可满足性公式 *F* 的子句中，不失一般性，证明了 *WP* 算法收敛情况下，确定的变元高概率的是骨干变元集，且骨干变元集高概率地包含于在这组赋值 φ^* 中，为定理 1 的证明提供了一定的条件。

5 结束语

本文从骨干集与后门集变量之间的关系引出了 *WP* -可解的概念，当随机产生的 3*CNF* 公式 *F* 为 *WP* -可解公式时，当且仅当 *WP* 算法高概率收敛。进一步研究：a)研究 *WP* -可解公式的结构性质、难解公式与 *WP* -不可解性；b)研究信息传播算法的依概率收敛性；c)研究 *WP* -可解的规则（3,4）-CNF 公式的结构性质、以该公式为输入的信息传播算法的收敛性和依概率收敛性。

参考文献：

[1] Dyer M, Frieze A, Molloy M. A probabilistic analysis of randomly generated binary constraint satisfaction [J]. Theoretical Computer Science, 2003, 290 (3): 1815-1828.

[2] Creignou N, Daudé H. The SAT–UNSAT transition for random constraint satisfaction problems [J]. Discrete Mathematics, 2009, 309 (8): 2085-2099.

[3] Gaspers S, Papadimitriou C, Sæther S H, *et al.* On satisfiability problems with a linear structure [J]. arXiv preprint arXiv: 1602. 07876, 2016.

[4] Doerr B, Neumann F, Sutton A M. Time complexity analysis of evolutionary algorithms on random satisfiable k-CNF formulas [J]. Algorithmica, 2017, 78 (2): 561-586.

[5] Sosa-Ascencio A, Ochoa G, Terashima-Marin H, *et al.* Grammar-based generation of variable-selection heuristics for constraint satisfaction problems [J]. Genetic Programming and Evolvable Machines, 2016, 17 (2): 119-144.

[6] Abbe E, Montanari A. Conditional random fields, planted constraint satisfaction and entropy concentration [M]// Approximation, Randomization, and Combinatorial Optimization Algorithms and Techniques. Berlin：Springer, 2013: 332-346.

[7] Alfredo B, Luca D, Guilhem S, *et al.* The large deviations of the whitening process in random constraint satisfaction problems [J]. Journal of Statistical Mechanics: Theory and Experiment, 2016, 2016 (5): 053401.

[8] Kirkpatrick S, Selman B. Critical behavior in the satisfiability of random boolean expressions [J]. Science, 1994, 264 (5163): 1297-1301.

[9] Kaporis A C, Kirousis L M, Lalas E G. The probabilistic analysis of a greedy satisfiability algorithm [J]. Random Structures & Algorithms, 2006, 28 (4): 444-480.

[10] Dubois O, Boufkhad Y, Mandler J. Typical random 3-SAT formulae and the satisfiability threshold [J]. arXiv preprint cs/0211036, 2002.

[11] Xu Ke, Boussemart F, Hemery F, *et al.* Random constraint satisfaction: easy generation of hard satisfiable instances [J]. Artificial Intelligence, 2007. 171 (8): 514-534.

[12] Xu Ke, Wei Li. Many hard examples in exact phase transitions [J]. Theoretical Computer Science, 2006, 355 (3): 291-302.

[13] Coja-Oghlan A, Panagiotou K. The asymptotic k-SAT threshold [J]. Advances in Mathematics, 2016, 288: 985-1068.

[14] Williams R, Gomes C P, Selman B. Backdoors to typical case complexity [C]// Proc of the 18th International Joint Conference on Artificial Intelligence. San Francisco, CA： Morgan Kaufmann Publishers Inc， 2003: 1173-1178.

[15] Kilby P, Slaney J, Thiébaux S, *et al.* Backbones and backdoors in satisfiability [C]// Proc of the 20th National Conference on Artificial Intelligence. Pennsylvania ：AAAI Press， 2005: 1368-1373.

[16] Hemaspaandra L A, Narváez D E. Search versus decision: the opacity of backbones and backdoors under a weak assumption [J]. arXiv preprint arXiv: 1706. 04582, 2017.

[17] Janota M, Lynce I, Marques-Silva J. Algorithms for computing backbones of propositional formulae [J]. AI Communications, 2015, 28 (2): 161-177.

[18] Gregory P, Fox M, Long D. A new empirical study of weak backdoors [C]// Proc of the 14th International Conference on Principles and Practice of Constraint Programming. Berlin：Springer, 2008: 618-623.

[19] Marques-Silva J， Janota M， Lynce I. On computing backbones of propositional theories [C]// Proc of the 19th European Conference on Artificial Intelligence. 2010: 15-20.

[20] Meier A, Ordyniak S, Ramanujan M S, *et al.* Backdoors for linear temporal logic [J]. Algorithmica, 2018, 81(2): 476-496..

[21] Zhou Huan, Xu Shouzhi, Ren Dong, *et al.* Analysis of event-driven warning message propagation in vehicular ad hoc networks [J]. Ad hoc Networks, 2017, 55: 87-96.

[22] Braunstein A, Mezard M, Zecchina R. Survey propagation: an algorithm for satisfiability [J]. Random Structures & Algorithms, 2005, 27 (2): 201-226.

[23] Krivelevich M, Vilenchik D. Solving random satisfiable 3CNF formulas in expected polynomial time [C]// Proc of the 17th annual ACM-SIAM symposium on Discrete algorithm. Society for Industrial and Applied Mathematics. Philadelphia, PA： Society for Industrial and Applied Mathematics，2006: 454-463.

[24] Feige U, Mossel E, Vilenchik D. Complete convergence of message passing algorithms for some satisfiability problems [M]// Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques. Berlin：Springer, 2006: 339-350.

[25] Abbe E, Montanari A. Conditional random fields, planted constraint satisfaction and entropy concentration [M]// Approximation,

Randomization, and Combinatorial Optimization. Algorithms and Techniques. Berlin ： Springer, 2013: 332-346.

[26] Wang Xiaofeng, Jiang Jiulei. Warning propagation algorithm for the MAX-3-SAT problem [J]. IEEE Trans on Emerging Topics in Computing, http://doi.org/10.1109/tetc.2017.2736504. 2017.

[27] 王晓峰，许道云. 警示传播算法收敛的充分条件 [J]. 软件学报，2016, 27 (12): 3003-3013. (Wang Xiaofeng, Xu Daoyun. Sufficient conditions for warning propagation algorithm convergence [J]. Journal of Software, 2016, 27 (12): 3003-3013.)

[28] Sutton A M, Neumann F. Runtime analysis of evolutionary algorithms on randomly constructed high-density satisfiable 3-CNF formulas [C]// Proc of International Conference on Parallel Problem Solving from Nature. [S.l.]:Springer International Publishing. 2014: 942-951.

[29] 王晓峰，许道云，秦永彬. 求解公式关键文字集的信息传播算法 [J]. 山东大学学报 :工学版 ，2011, 41 (3): 1-6. (Wang Xiaofeng, Xu Daoyun, Qin Yongbin. Information propagation algorithm for solving key word sets of formulas [J]. Journal of Shandong University :Engineering Edition , 2011, 41 (3): 1-6.)